CYBER RESILIENCE PLATFORM

SECURE BY EVIDENCE

TECHNISCHE FUNKTIONEN / VERTRAULICH

AA-sec: Funktionen & Sicherheit

CRA-Compliance automatisieren. Kontrolle behalten. Jeden Schritt belegen.

WER SIND WIR

Für Engineering und QA-getriebene Entwicklung

Anton C.

QA Lead
Prozessautomatisierung Profi
MCP-Experte

Anton V.

Architekt für sicherheitskritischer Systeme
Cybersecurity-Spezialist
Embedded Engineer

Warum wir: Erfahrung aus sicherheitskritischen Systemen. QA-getriebene Prozesse. Nachweise von Anfang an. Von Praktikern für Praktiker.

DAS PROBLEM

Nachweise gehören nicht in Tabellen.

Heute

Nachweise liegen oft verteilt in Tools, Repositories, Tickets und Dokumenten.
Für Audits oder Reviews müssen Teams sie manuell zusammenführen.

Ziel

Security-Nachweise automatisieren –
mit einfachen Integrationen, integrierten Scans und fertigen Workflows. So bleibt der Nachweisstand aktuell, ohne eine eigene Compliance-Plattform zu bauen.

PLATTFORMÜBERBLICK

Eine Plattform für den gesamten CRA & Security-Lifecycle

Produkte verwalten, Compliance automatisieren, Änderungen überwachen, Nachweise aktuell halten.

Organisation & Zugriff

Nutzer, Rollen, Rechte

Produkte & Releases

Produkte, Teilprodukte, Versionen

CRA Assessment

Anforderungen, Compliance-Status

SBOM & Schwachstellen

Komponenten, Quellen, Analyse

Post-Market & Art. 14

Monitoring, Melde-Workflows

Nachweise & Historie

Herkunft, Änderungen, Aktivitäten

Dokumente

Vorlagen, Dossiers, Generierung

Integrationen

APIs, Standard & Custom

Security by Design

Datenisolation · Kryptografie · Dezentrales Recovery

ORGANISATION & ZUGRIFF

Teams organisieren. Zugriff steuern.

Organisation einrichten, Zuständigkeiten definieren und Zugriffe steuern.

Organisation

Daten und Struktur verwalten.

Benutzer & Teams

Nutzer hinzufügen und Teams organisieren.

Rollen & Berechtigungen

Zuständigkeiten und Berechtigungen festlegen.

Sichtbarkeit

Nur freigegebene Produkte und Daten sehen.

PRODUKTE & RELEASES

Produkte modellieren. Releases verwalten.

Produkte und Teilprodukte strukturieren, Versionen und Releases zentral steuern.

Produktstruktur

Produkte als Basis des CRA-Lifecycle anlegen.

Teilprodukte

Komplexe Produkte in verbundene Teilprodukte und Komponenten gliedern.

Versionen

Entwicklung über Versionen hinweg verfolgen.

Releases

Releases mit eigenem Produkt- und Compliance-Kontext verwalten.

LIFECYCLE-MODELL

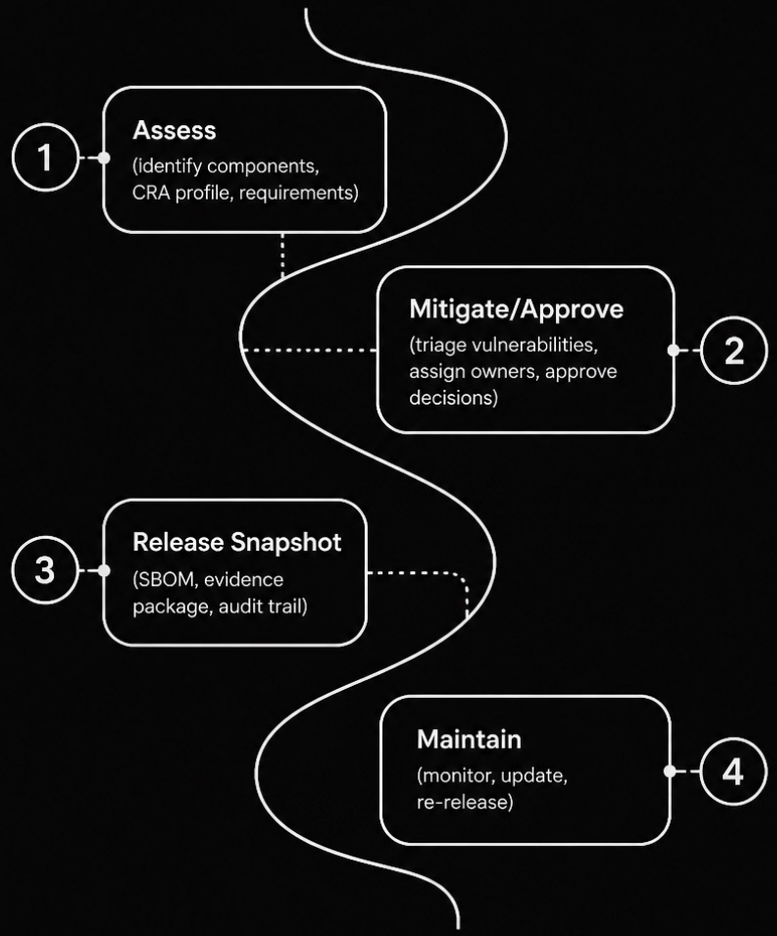
Produkt & Release: zwei Ebenen, ein Lifecycle

Produkt = laufender Kontext

Identität, Verantwortliche, Komponenten, Anforderungen, CRA-Profil, Verwendungszweck und Zuständigkeiten – laufend gepflegt.

Release = prüfbarer Snapshot

Definierter Versionsstand mit SBOM, Schwachstellenstatus, Entscheidungen, Nachweisen, Dokumenten und Audit Trail.



CRA ASSESSMENT

Anforderungen bewerten. Compliance im Blick behalten.

CRA-Anforderungen strukturiert bewerten und den Status jedes Produkts jederzeit sehen.

Relevante Anforderungen

Nur die für das Produkt relevanten CRA-Anforderungen.

Strukturiertes Assessment

Konsistenter, wiederholbarer Prüfprozess.

Compliance-Status

Erledigt, offen oder ohne Nachweis – auf einen Blick.

Laufender Lifecycle

Bewertungen bleiben mit Produkt, Versionen und Daten aktuell.

SBOM & SCHWACHSTELLEN

Wissen, was drin ist.
Wissen, was verwundbar ist.

SBOMs strukturieren und laufend gegen angebundene Schwachstellenquellen prüfen.

SBOM-Verarbeitung

SBOMs importieren und in den Produkt-Lifecycle übernehmen.

Komponenten

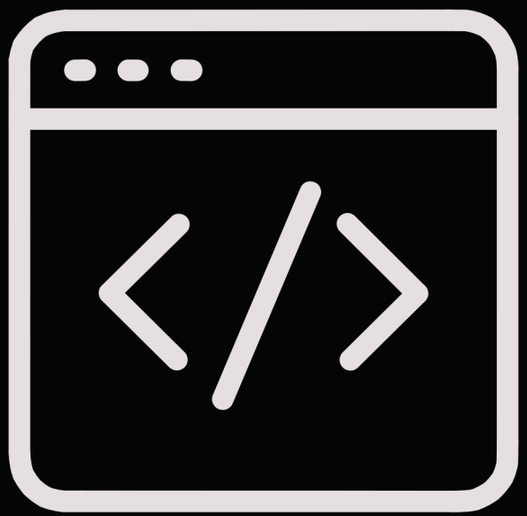
Softwarekomponenten je Produkt und Release verwalten.

Schwachstellenanalyse

Komponenten mit Schwachstellendaten abgleichen und Findings verfolgen.

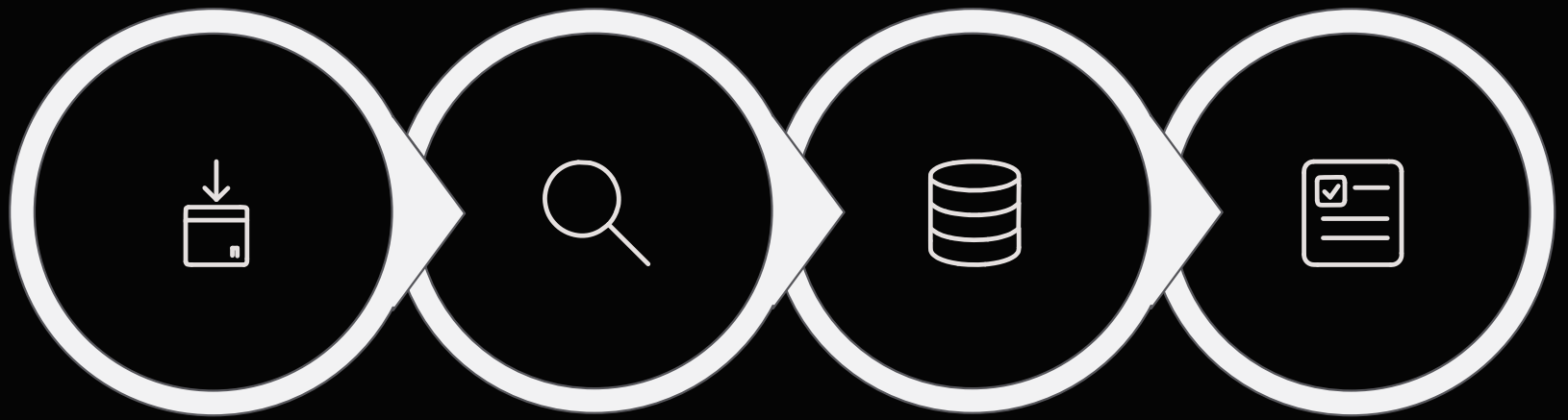
Erweiterbare Quellen

Mehrere Datenbanken anbinden und neue Quellen ergänzen.



SBOM & SCANNER

Integrierter Scanner & SBOM-Pipeline



SBOM ist in AA-sec ein zentrales Produktsicherheitsobjekt. Externe Scanner, CI/CD, SBOM-Exporter und Vulnerability-Quellen liefern Daten über Normalizer; AA-sec verwaltet den normalisierten Sicherheitsstatus und den Evidence Trail.

POST-MARKET & ARTIKEL 14

Nach Release überwachen. Rechtzeitig reagieren.

Freigegebene Produkte laufend überwachen und relevante Security Events in Artikel-14-Workflows überführen.

Monitoring

Produkte und bekannte Komponenten laufend auf neue Schwachstellen prüfen.

Relevante Änderungen

Erkennen, wenn neue Informationen ein bestehendes Produkt oder Release betreffen.

Artikel-14-Workflows

Maßnahmen und Meldungen strukturiert steuern.

Alerts & Fristen

Verantwortliche informieren und kritische Fristen im Blick behalten.

ARTIKEL 14

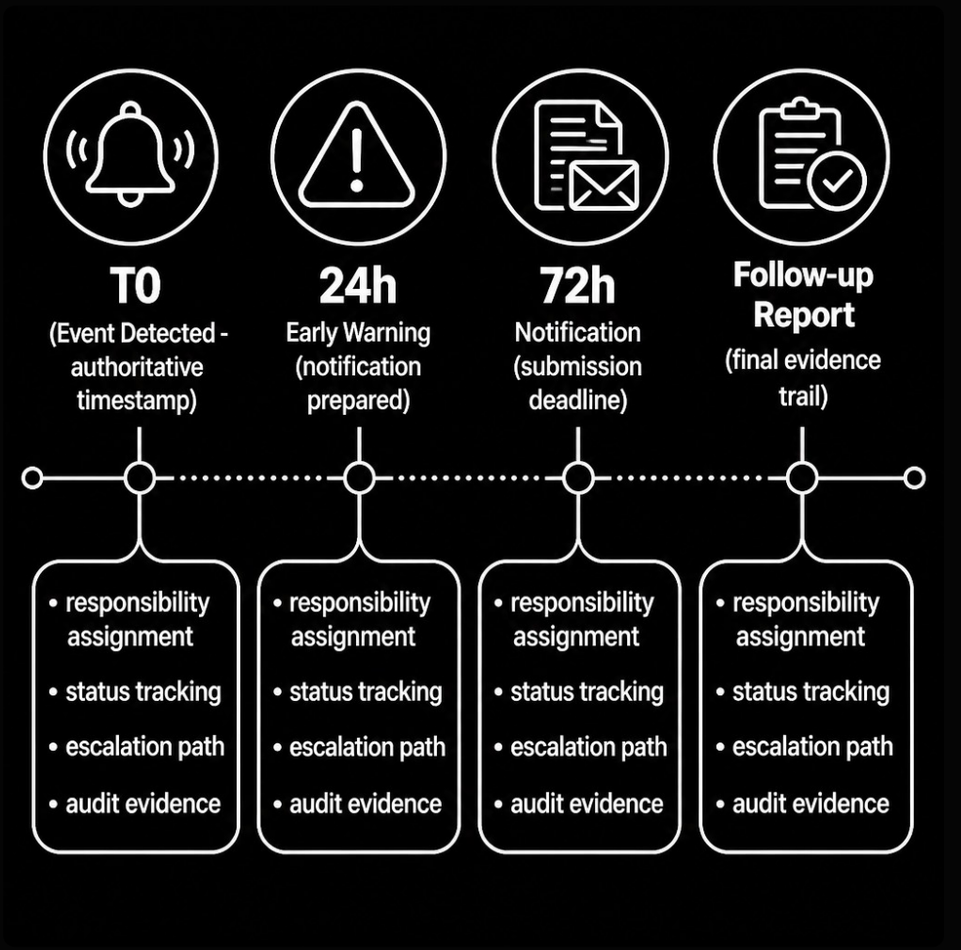
CRA Article 14 Workflow

Fristen werden als Status und Zeitpunkte gespeichert – nicht als fragile In-Memory-Timer. Neustarts oder Deployments verlieren keine Pflichten.

Ablauf

- **T0:** Ereignis erkannt – Startzeit gesetzt
- **24h:** Early Warning
- **72h:** Meldung fällig
- **Follow-up:** Abschlussbericht verfolgen

Geplante Checks prüfen Fristen und Workflow-Status. Zuständigkeit, Status, Blocker, Eskalation und Einreichungsnachweise bleiben gespeichert.



NACHWEISE & HISTORIE

Nachweise sichern. Änderungen nachvollziehen.

Eine lebende Nachweisbasis je Produkt – verknüpft mit Anforderungen, Releases, Assessments und Historie.

Nachweise

Informationen und Artefakte zur Produkt-Compliance erfassen.

Verknüpfungen

Nachweise mit Produkt, Release, Anforderung und Assessment verbinden.

Herkunft

Quelle und Entstehungskontext festhalten.

Historie

Relevante Aktionen und Änderungen nachvollziehbar speichern.

DOKUMENTE

Dokumente aus aktuellen Compliance-Daten.

Produktdaten und Nachweise mit flexiblen Vorlagen in konsistente, nachvollziehbare Dokumente überführen.

Inhalt und Design bleiben flexibel – die Verbindung zu den Quelldaten bleibt erhalten.

Automatische Generierung

Dokumente und Dossiers direkt aus Plattformdaten.

Flexible Vorlagen

Struktur und Inhalt je Organisation anpassen.

Eigenes Design

Branding und Layout frei gestalten.

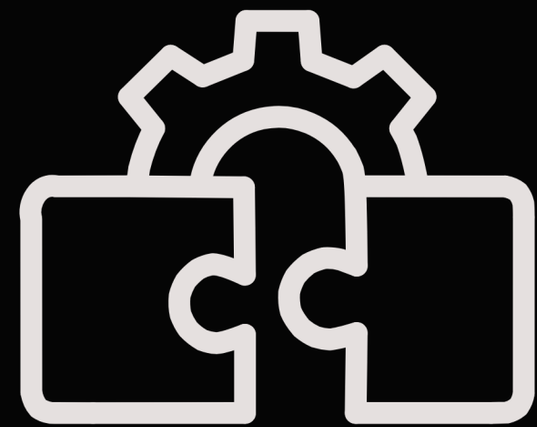
Nachweisbare Herkunft

Inhalte bleiben mit Quellen und Nachweisen verknüpft.

INTEGRATIONEN & AUTOMATISIERUNG

Toolchain anbinden. Workflows automatisieren.

AA-sec in bestehende Tools und Prozesse integrieren – über Standardintegrationen, APIs und individuelle Schnittstellen.



Standardintegrationen

Gängige Engineering- und Security-Tools anbinden.

API

Plattformfunktionen aus bestehenden Systemen und Pipelines automatisieren.

Custom Integrations

Eigene Tools und Prozesse anbinden.

Workflow-Automatisierung

Daten und Aktionen ohne manuelle Übergaben austauschen.

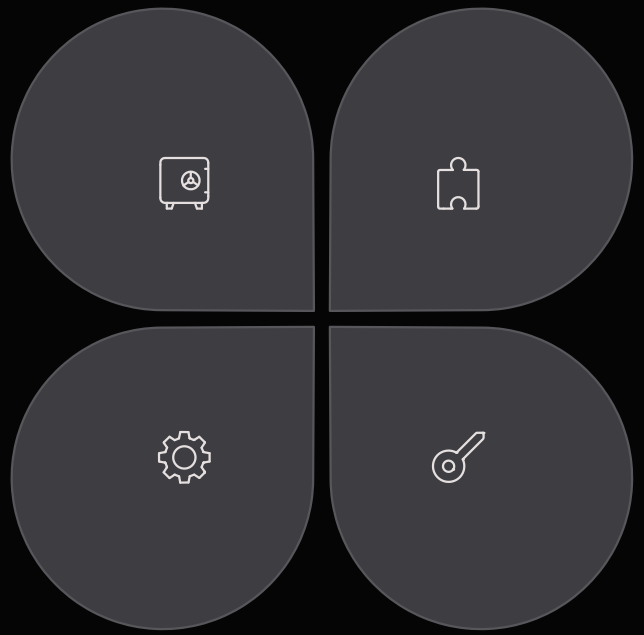
KRYPTOGRAFIE & RECOVERY

Verschlüsselung by Design.
Recovery ohne zentrale Vertrauensinstanz.

Organisationsdaten kryptografisch schützen und Recovery dezentral absichern.

Verschlüsselung je Organisation

Sensible Daten bleiben im kryptografischen Kontext der Organisation.



Getrennte Vertrauensbereiche

Kein universeller Schlüssel und kein zentraler Trust Point.

Teil der Plattform

Verschlüsselung und Recovery sind fest eingebaut.

Dezentrales Recovery

Wiederherstellung über ein verteiltes Modell statt eines Master-Schlüssels.

WORKFLOW-FLEXIBILITÄT

UI

Direkt im UI

Produkte, Assessments, Nachweise und Dokumente direkt in AA-sec verwalten.

Geführte Workflows

Strukturierte Abläufe für die tägliche Compliance-Arbeit.

Alles im Blick

Produkte, Assessments, Nachweise und Status zentral sehen.

Im Team

Rollenübergreifend mit kontrolliertem Zugriff arbeiten.

Sofort starten

Keine eigene Automatisierung nötig.

API

Per API automatisieren

AA-sec in bestehende Engineering-, Security- und Compliance-Prozesse integrieren.

Automation

Aktionen aus Systemen und Pipelines auslösen.

Integration

Daten mit Tools und internen Workflows austauschen.

Eigene Prozesse

AA-sec an Ihre Toolchain anpassen.

Skalieren

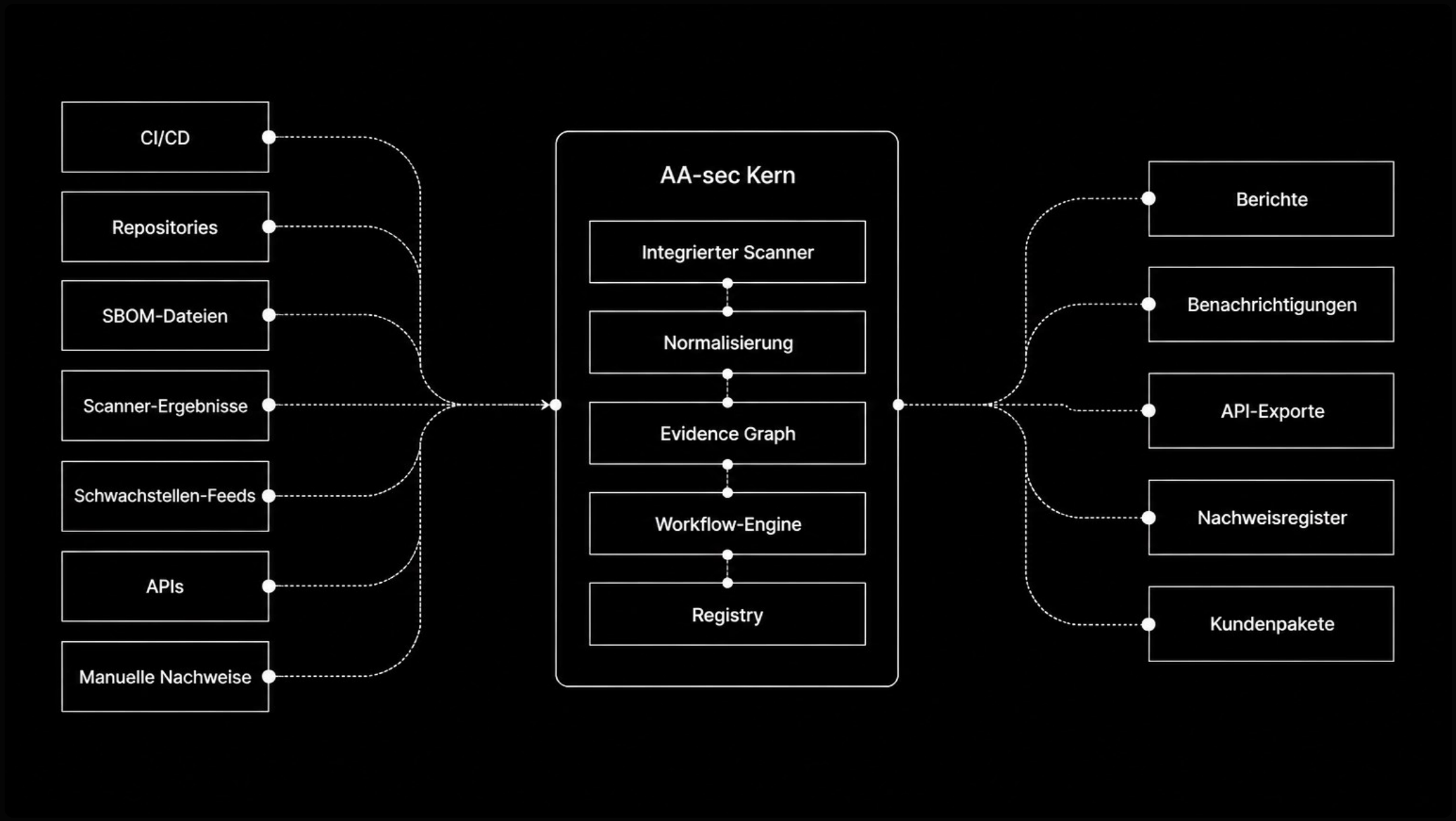
Wiederkehrende Abläufe automatisieren.

UI, API – oder beides zusammen.

INTEGRATION

Integrationsarchitektur

AA-sec verbindet unterschiedliche Datenquellen, verarbeitet sie einheitlich und stellt Ergebnisse flexibel bereit – passend zu Ihrer Toolchain.



Betriebsmodi

Scanner-First

Kein eigener Scanner-Stack nötig: AA-sec übernimmt Dependency- und Vulnerability-Scanning.

Connector

Bestehende Scanner und Tools liefern Daten an AA-sec.

Output-Only

API/MCP lesen Ergebnisse und Nachweise, ohne den Compliance-State zu übernehmen.

MCP

Nutzen Sie Ihren eigenen KI-Agenten.

Über MCP erhält Ihr Agent strukturierten Zugriff auf Produkt-, Compliance- und Nachweiskontext.

Ihr KI-Agent

MCP

AA-sec Plattform

Strukturierter Kontext

Produkt-, Compliance-, Schwachstellen- und Nachweisdaten maschinenlesbar nutzen.

Gleiche Zugriffsgrenzen

Der Agent arbeitet innerhalb derselben Rollen und Berechtigungen.

Ihr KI-Stack

Modell, Agentenarchitektur und Workflow bleiben Ihre Entscheidung.

MCP stellt Plattformkontext bereit.

Dateneingang und Schreibzugriffe bleiben auf dem Integrations-/API-Pfad.

Self-hosted Telemetrie: nur Opt-in.

PRODUKT-LIFECYCLE

Compliance endet nicht mit dem Release.

AA-sec begleitet Ihr Produkt durch den gesamten Lifecycle – von der Definition über den Betrieb bis zum nächsten Release.

Produkt
Anlegen

Bewertung
CRA, SBOM, Schwachstellen

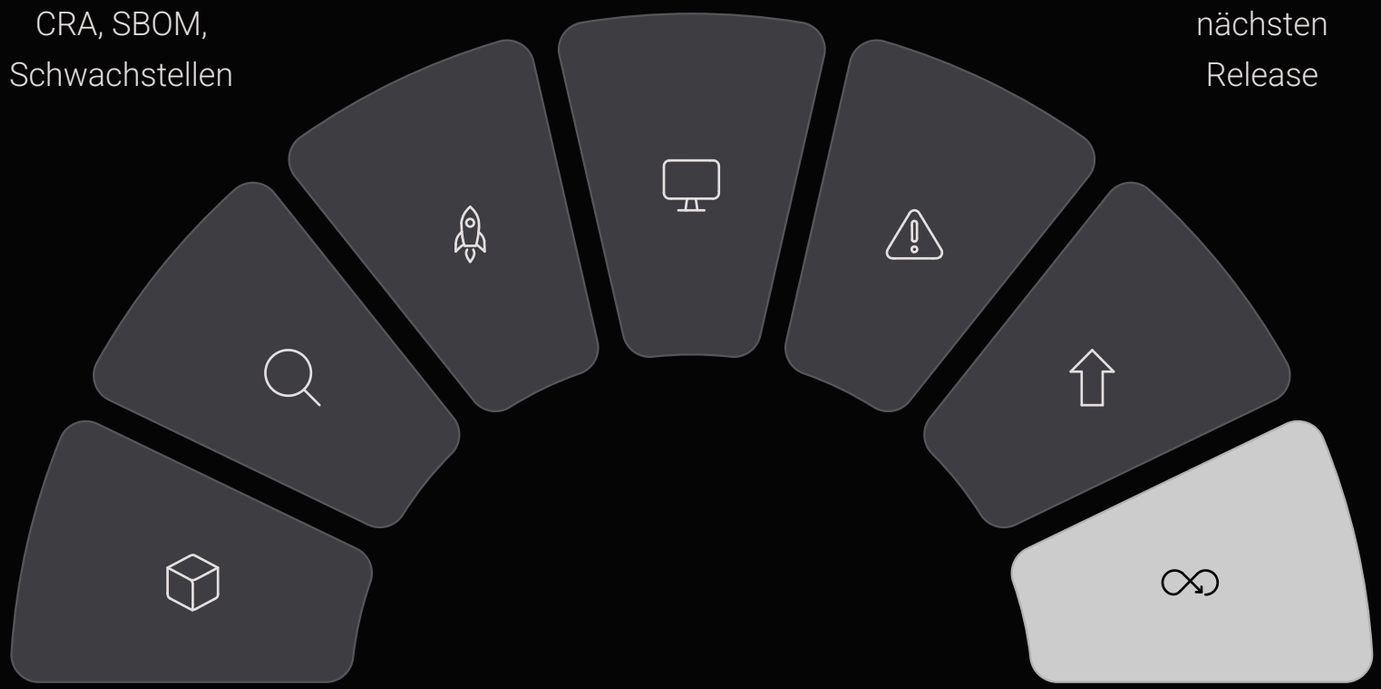
Release
Vorbereiten & freigeben

Monitoring
Laufend überwachen

Reaktion
Auf Änderungen reagieren

Update
Für den nächsten Release

Repeat
Auch in 10 Jahren



Nachweise wachsen mit. Dokumente entstehen aus dem aktuellen Stand.

Was heute belegt ist, bleibt auch morgen nachvollziehbar.

BETRIEB

Zuverlässigkeit & Betrieb

AA-sec hält Compliance-Daten dauerhaft konsistent und kritische Workflows robust gegen Neustarts und Ausfälle.

Persistenter Zustand

Fristen, Findings, Workflow-Status, Nachweise und Artefakte werden dauerhaft gespeichert.

Queue-Verarbeitung

Lange Jobs laufen asynchron mit Retry-Logik.

Restart-safe

Artikel-14-Workflows und Dokumentgenerierung hängen nicht an laufenden Sessions.

Idempotent

Wiederholte Jobs erzeugen keine doppelten Events oder Datensätze.

Operational Visibility

Logs, Health Checks, Status-APIs und Audit Events machen Betrieb und Fehler sichtbar.

Kontrollierte Änderungen

DB-, Schema- und Release-Änderungen schützen historische Compliance-Daten.

Ergebnis: Pflichten und Nachweise bleiben auch bei Worker-Ausfällen, Neustarts oder Verzögerungen erhalten.

BEREITSTELLUNG

Ihre Umgebung. Unsere Plattform. Gemeinsam.

Für hohe Anforderungen an Infrastrukturkontrolle und Datenresidenz bieten wir ein On-Premise-Paket.

In Ihrer Umgebung

AA-sec läuft in Ihrer kontrollierten Infrastruktur. Deployment und Daten bleiben bei Ihnen.

Ihre Systeme

Identity Provider, Storage, Security-Tools und interne Prozesse integrieren wir mit.

Gemeinsam starten

Wir unterstützen bei Konfiguration, Integration, Validierung und den ersten Workflows.

Ziel: AA-sec passt sich Ihrem Betriebsmodell an – nicht umgekehrt.

BEREITSTELLUNG

Deployment-Modelle & Vertrauensgrenzen

Flexible Optionen für unterschiedliche Anforderungen an Kontrolle, Compliance und Infrastrukturisolation.

AA-sec EU SaaS

VERFÜGBAR

Primäres Angebot. AA-sec übernimmt Hosting, Deployment, Updates und Betrieb. Datenhaltung in der EU.

As it is.

Dedicated Deployment

GEPLANT

Eigene Kundenumgebung für stärkere Isolation und besondere Security- oder Procurement-Vorgaben.

Für anspruchsvolle IT-Vorgaben.

On-Premise

NICHT BEGONNEN

Betrieb direkt in Ihrer Infrastruktur. Aktuell Konzept, noch nicht in Entwicklung.

Auf Ihre Umgebung zugeschnitten.

Das Deployment ändert den Betriebsort – nicht Nachweismodell, Workflows oder Audit-Logik.

ENTWICKLUNGSSTATUS

Stand der Entwicklung

Kernfunktionen sind umgesetzt. Offen sind vor allem UI, externe Integrationen und das On-Premise-Paket.

BEREIT

- Produkt-Lifecycle
- Release-/State-Modell
- Scanner & Dependency-Scanning
- SBOM-Modell & Governance
- Vulnerability-Workflow
- CRA Article 14 Workflow
- Dokumente & Dossiers
- Tenant-Isolation & Verschlüsselung
- Nachweisintegrität & Audit Trail

TEILWEISE

- UI
- Externe Integrationen

NICHT BEGONNEN

- On-Premise-Paket

BEREIT = Kernfunktion vorhanden und nutzbar; UI und Enterprise-Paket können noch unvollständig sein.

CYBER RESILIENCE PLATFORM

SECURE BY EVIDENCE

Integrierter Scanner.

Evidence Graph.

Workflow-Verantwortung.

AA-sec macht aus Produktsicherheitsarbeit strukturierte, nachvollziehbare Nachweise – über Produkte, Releases, Schwachstellen, CRA-Workflows und Dokumente hinweg.

TECHNISCHE FUNKTIONEN / VERTRAULICH